English Translation of Relevant Portions of JP-A-2001-148735
Published on May 29, 2001

:

:

Page (9), column 15, line 48 – column 16, line 15

[0085] The above description deals with the case where the clock of the transmitting terminal and that of the decoder module show the same time. However, when something causes an error to occur between the time shown by the clock of the transmitting terminal and that shown by the clock of the decoder module, it may become impossible for the decoder module to perform decryption.

[0086] In a ninth embodiment of the present invention shown in Fig. 12, a description will be given of a decryption validity check mechanism that solves the problem (i.e., the impossibility of decryption) resulting from an error between the time shown by the clock of the transmitting terminal and that shown by the clock of the decoder module.

[0087] In this embodiment, for a predetermined period after a key change, an old work key used before the key change as well as a new work key used after the key change is held at the decoder module side such that both is available. In this case, decryption is performed using both the old and new work keys (in Fig. 12, (1) decryption and (2) decryption), the decryption results are compared according to "a post-decryption validity check method" using verification data (Fig. 12, (4) comparison and verification), and the correctly decrypted one of the decryption results is transmitted as location data (Fig. 12, (5) location data

transmission).

:

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-148735
(43)Date of publication of application : 29.05.2001

(51)Int.Cl. H04M 3/42
H04L 9/08
H04L 9/14
H04M 3/487
H04M 11/00

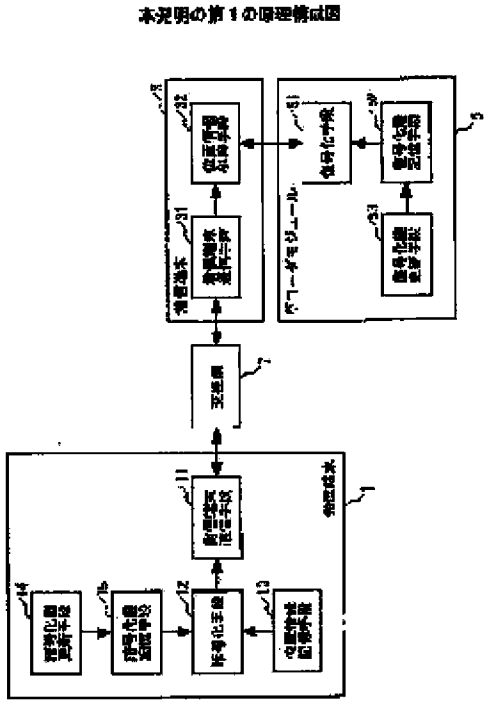
(21)Application number : 2000-081961
(22)Date of filing : 23.03.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MASUDA RYUTA
DATE SHIGERU
YASUNAGA KENJI
MINE SHINICHI

(30)Priority
Priority number : 11253640 Priority date : 07.09.1999 Priority country : JP

(54) POSITION INFORMATION SERVICE SYSTEM, POSITION INFORMATION USING METHOD OF POSITION INFORMATION SERVICE SYSTEM, ORIGINATING TERMINAL, AND DECODER MODEL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a position information service system which makes the ID of an originating terminal secret to the outside of an exchange network, provides information for a terminating terminal unlimited to a special number and charges the terminal, and prevent position information from being altered and data from illegally being reused.
SOLUTION: The originating terminal stores position information, ciphers the position information by using a ciphering key which is periodically updated, and sends the information to a decoder module attached to a terminating terminal. The decoder module deciphers the ciphered position information by using a deciphering key which is automatically updated when the ciphering key of the originating terminal is updated and provides the information for the terminating terminal. The originating terminal generates a key including the terminating terminal telephone number and ciphers the position information and the decoder module generates a key including the telephone number of the connected terminating terminal, so that only the limited terminal obtains the position information deciphered by the decoder module.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－148735
(P2001－148735A)
(43)公開日　平成13年５月29日(2001.5.29)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
H04M	3/42		H04M	3/42	U	5J104
H04L	9/08			3/487		5K015
	9/14			11/00	302	5K024
H04M	3/487		H04L	9/00	601C	5K101
	11/00	302			641	

審査請求　未請求　請求項の数15　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－81961(P2000－81961)
(22)出願日　平成12年３月23日(2000.3.23)
(31)優先権主張番号　特願平11－253640
(32)優先日　平成11年９月７日(1999.9.7)
(33)優先権主張国　日本（ＪＰ）

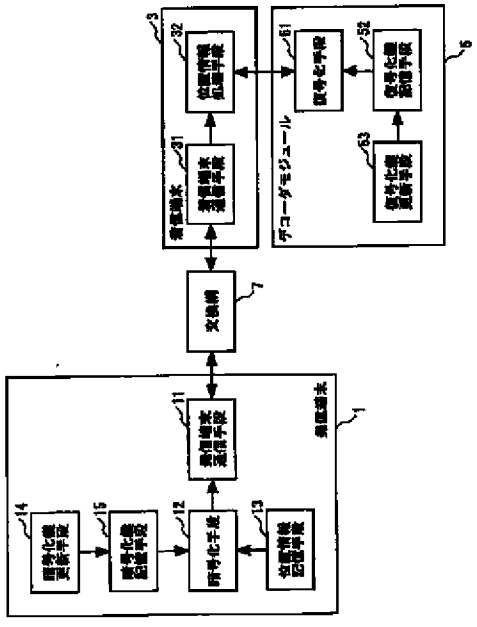
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　増田　竜太
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　伊達　滋
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　位置情報サービスシステム、並びに、位置情報サービスシステムにおける位置情報利用方法、発信端末、及び、デコーダモジュール

(57)【要約】
【課題】　本発明は、発信端末のＩＤが交換機網外に秘匿され、特番に限定されない着信端末に情報提供及び課金が行なわれ、位置情報の改竄、データの不正な再利用が防止された位置情報サービスシステムの提供を目的とする。
【解決手段】　本発明によれば、発信端末は、位置情報を記憶し定期的に更新される暗号化鍵を使って位置情報を暗号化して着信端末に付属されたデコーダモジュールに送信する。デコーダモジュールは、発信端末の暗号化鍵更新時に自動更新される復号化鍵を使って暗号化位置情報を復号化し着信端末に提供する。発信端末で着信端末電話番号を入れた鍵を生成して位置情報を暗号化し、デコーダモジュールで接続された着信端末の電話番号を入れた鍵を生成することで、限定された着信端末だけがデコーダモジュールで復号化された位置情報を得る。

本発明の第１の原理構成図



1

【特許請求の範囲】

【請求項１】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおいて、

上記発信端末で、暗号化鍵及び上記着信端末の識別情報を用いて上記位置情報を暗号化する段階と、

上記発信端末で、上記暗号化された位置情報を上記交換網を介して上記着信端末に送信する段階と、

上記着信端末に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を保持するデコーダモジュールで、上記着信端末に受信された上記暗号化された位置情報を上記復号化鍵を用いて復号化する段階と、

上記着信端末で、上記復号化された位置情報を処理する段階とを有し、

上記発信端末の暗号化鍵と上記デコーダモジュールの上記復号化鍵が所定の時点で同期して更新され、上記デコーダモジュールが取り付けられた着信端末において上記発信端末の位置情報を利用することができる位置情報利用方法。

【請求項２】　上記暗号化鍵を用いて位置情報を暗号化する段階は、

上記暗号化鍵及び上記着信端末の識別情報を用いてワーク鍵を作成する段階と、

上記ワーク鍵を用いて上記位置情報を暗号化する段階とを有し、

上記デコーダモジュールに保持された上記復号化鍵は、上記更新された暗号化鍵及び上記デコーダモジュールが取り付けられている上記着信端末の識別情報を用いて更新される請求項１記載の位置情報利用方法。

【請求項３】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムであって、

上記発信端末は、暗号化鍵及び上記着信端末の識別情報を用いて上記位置情報を暗号化する手段と、

上記暗号化鍵を所定の時点で更新する手段と、

上記暗号化された位置情報を上記交換網を介して上記着信端末に送信する手段とを有し、

上記着信端末に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を保持する手段、

上記着信端末に受信された上記暗号化された位置情報を上記復号化鍵を用いて復号化する手段、及び、上記暗号化鍵が更新される所定の時点と同期して上記復号化鍵を更新する手段を備えたデコーダモジュールが設けられ、

上記着信端末は上記復号化された位置情報を処理する手段を有し、

上記デコーダモジュールが取り付けられた上記着信端末において上記発信端末の位置情報を利用することができる位置情報サービスシステム。

2

【請求項４】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおける発信端末の位置情報利用方法であって、

暗号化鍵及び上記着信端末の識別情報を用いて上記位置情報を暗号化する段階と、

上記暗号化された位置情報を上記交換網を介して上記着信端末に送信する段階と、

上記着信端末に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を保持し、上記暗号化された位置情報を上記復号化鍵を用いて復号化するデコーダモジュールで、上記復号化鍵が更新される時点に同期して上記暗号化鍵を更新する段階とを有する、位置情報利用方法。

【請求項５】　上記暗号化鍵を用いて位置情報を暗号化する段階は、

上記暗号化鍵及び上記着信端末の識別情報を用いてワーク鍵を作成する段階と、

上記ワーク鍵を用いて上記位置情報を暗号化する段階とを有し、

上記デコーダモジュールに保持された上記復号化鍵が上記更新された暗号化鍵及び上記デコーダモジュールが取り付けられている上記着信端末の識別情報を用いて更新される請求項４記載の位置情報利用方法。

【請求項６】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおいて、

暗号化鍵及び上記着信端末の識別情報を用いて上記位置情報を暗号化する手段と、

上記着信端末に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を用いて、上記着信端末に受信された上記暗号化された位置情報を復号化するデコーダモジュールで上記復号化鍵が更新される所定の時点と同期して上記暗号化鍵を更新する手段と、

上記暗号化された位置情報を上記交換網を介して上記着信端末に送信する手段とを有する発信端末。

【請求項７】　上記暗号化する手段は、上記暗号化鍵及び上記着信端末の識別情報を用いてワーク鍵を作成する手段と、

上記ワーク鍵を用いて上記位置情報を暗号化する手段とを有する請求項６記載の発信端末。

【請求項８】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおいて、上記発信端末に搭載される位置情報利用プログラムを格納した記録媒体であって、

暗号化鍵及び上記着信端末の識別情報を用いて上記位置

情報を暗号化させるプロセスと、
上記着信端末に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を用いて、上記着信端末に受信された上記暗号化された位置情報を復号化するデコーダモジュールで上記復号化鍵が更新される所定の時点と同期して上記暗号化鍵を更新させるプロセスとを有する位置情報利用プログラムを格納した記録媒体。

【請求項９】　上記暗号化させるプロセスは、上記暗号化鍵及び上記着信端末の識別情報を用いてワーク鍵を作成させるプロセスと、
上記ワーク鍵を用いて上記位置情報を暗号化させるプロセスとを有する請求項８記載の位置情報利用プログラムを格納した記録媒体。

【請求項１０】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおいて着信端末に取り付けられたデコーダモジュールの位置情報利用方法であって、
上記発信端末で暗号化鍵及び上記着信端末の識別情報を用いて暗号化され、上記交換網を介して上記着信端末に送信された暗号化位置情報を、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を用いて復号化する段階を有し、
上記発信端末で上記暗号化鍵が更新される所定の時点と同期して、上記復号化鍵を更新する段階をさらに有する位置情報利用方法。

【請求項１１】　上記復号化鍵は、上記暗号化鍵及び上記着信端末の識別情報を用いて作成されたワーク鍵を使って暗号化された上記暗号化鍵位置情報を復号化できるように、上記更新された暗号化鍵及び上記着信端末の識別情報を用いて更新される請求項１０記載の位置情報利用方法。

【請求項１２】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおいて、着信端末に取り付けられたデコーダモジュールであって、
上記発信端末で暗号化鍵及び上記着信端末の識別情報を用いて暗号化され、上記発信端末に送信された暗号化位置情報を、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を用いて復号化する手段と、
上記復号化鍵を保持する手段と、
上記暗号化鍵が更新される所定の時点と同期して上記復号化鍵を更新する手段とを有するデコーダモジュール。

【請求項１３】　上記復号化鍵を更新する手段は、上記暗号化鍵及び上記着信端末の識別情報を用いて作成されたワーク鍵を使って暗号化された上記暗号化鍵位置情報を復号化できるように、上記更新された暗号化鍵及び上記着信端末の識別情報を用いて上記復号化鍵を更新する請求項１２記載のデコーダモジュール。

【請求項１４】　交換網と、上記交換網を介して接続された発信端末及び着信端末とを有し、上記発信端末の所在を表わす位置情報を上記着信端末に提供する位置情報サービスシステムにおいて、着信端末に取り付けられたデコーダモジュールに搭載される位置情報利用プログラムを格納した記録媒体であって、
上記発信端末で暗号化鍵及び上記着信端末の識別情報を用いて暗号化され、上記発信端末に送信された暗号化位置情報を、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を用いて復号化させるプロセスと、
上記暗号化鍵が更新される所定の時点と同期して上記復号化鍵を更新させるプロセスとを有する位置情報利用プログラムを格納した記録媒体。

【請求項１５】　上記復号化鍵を更新させるプロセスは、上記暗号化鍵及び上記着信端末の識別情報を用いて作成されたワーク鍵を使って暗号化された上記暗号化鍵位置情報を復号化できるように、上記更新された暗号化鍵及び上記着信端末の識別情報を用いて上記復号化鍵を更新させる請求項１４記載の位置情報利用プログラムを格納した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、公衆電話機のような発呼端末（又は発信端末）の設置場所を被呼端末（又は着信端末）に通知する位置情報サービスシステムに係わり、特に、位置情報サービスシステムのセキュリティを保障する技術に関する。

【０００２】

【従来の技術】従来、発信者の住所などの位置情報を着信者に提供するサービスとして、警察・消防回線のような特別な電話番号の着信者に対する発信地紹介サービスが提案されている（特開平08-204835）。このサービスでは、発信者の発呼端末の電話番号又は端末ＩＤを利用してセンタで位置情報を獲得し、着信者に位置情報を提供する。

【０００３】また、特開平08-204841には、発信者が公衆電話機を用いて自分の現在位置を相手に知らせるとともに、発信者自身も現在位置情報を得ることができる公衆電話位置情報システムが開示されている。このシステムでは、発信者が公衆電話機の電話番号や識別コードを基地局（センタ）へ送信し、基地局はこの発信者から送信された情報に基づいて位置情報を検索し、検索結果を受信局に送信する。位置情報の具体例には、所在地名、地図表示が含まれる。

【０００４】また、近年開始された発信者番号通知サービスを利用することにより、交換網の外部でも発信者の電話番号を知ることが可能になるので、電話番号とその電話番号に関連した位置情報とを対応付けしたデータベースなどを構築して発信者の位置情報を提供できるよう

になる。

【０００５】一方、位置情報サービスの円滑な運用のためには、利用者が望む適切な情報を提供できるだけではなく、一般に、サービス料の適切な課金が必要であると考えられる。さらに、サービス料の適切な課金を行なうため、サービスに関連した情報の秘匿性の向上や情報の改竄の防止などの情報セキュリティ技術が重要になる。

【０００６】従来技術における位置情報サービスへの課金方式として、たとえば、特開平10-326075に記載された発明によれば、ＩＣカード対応のデジタル公衆電話機を利用してその公衆電話機周辺の店舗等の行き先案内サービスを提供する方法において、公衆電話機からサービスセンタにダイヤルした際の通話料がＩＣカードや現金から清算される。

【０００７】

【発明が解決しようとする課題】上記の従来技術の説明からわかるように、発信者の発信端末の端末ＩＤ、たとえば、電話番号を知ることができる場合、電話番号をインデックスとした位置情報データベースを構築することにより、交換網の内外を問わずに発信端末の設置場所に関する位置情報を提供することができる。しかし、発信端末の電話番号は、一般には、発信者番号通知サービスを利用しない限り、着信者が知ることのできない情報であり、実際、電話番号を非通知・非公開としている加入者端末が数多く存在する。さらに、公衆電話機においては、その電話番号は非公開とされる。

【０００８】また、サービス提供者が電話番号をインデックスとして位置情報データベースを構築した場合、サービス利用者がサービス利用時に電話番号と位置情報の対を蓄積することによって、サービス提供者の位置情報データベースのサブセットを構築することが可能である。その場合、サービス利用者は、一旦サービスを利用した電話番号と同じ電話番号については、サービス提供者からのサービスを受けずに位置情報を取得でき、サービス提供者はサービス利用者に対し位置情報の利用料を適正に課金できない。

【０００９】したがって、本発明は、発信端末の電話番号の秘密性を保ったまま発信端末の設置場所を着信端末に通知する位置情報サービスシステムの提供を目的とする。

【００１０】また、本発明は、サービス利用者に適正な課金が行なえるように、デコーダモジュールのような付属装置を取り付けることによってサービス利用の許可を与えられた着信端末だけがサービスを利用できる位置情報提供サービスシステムの提供を目的とする。

【００１１】さらに、本発明は、位置情報利用の際に通信の負荷が発生しないように、着信端末がサービス提供者に問い合わせを行なうことなく位置情報サービスを受けることができるシステムの提供を目的とする。

【００１２】さらに、本発明は、サービス提供者と契約を締結していない不正な着信端末が不正にサービスを利用できないようなシステムの提供を目的とする。

【００１３】また、本発明は、上記位置情報サービスシステムにおける位置情報利用方法、発信端末、並びにデコーダモジュールの提供を目的とする。

【００１４】

【課題を解決するための手段】上記の目的を達成するため、本発明によれば、発信端末に位置情報を保持し、位置情報取得時に交換機網外で発信端末のＩＤ（電話番号）を使用しない。また、復号化サービスを受ける着信者は、デコーダモジュールを着信端末に取り付ける必要がある。

【００１５】さらに、本発明によれば､着信端末として特番を使用しない。また、位置情報は暗号化される｡その上、本発明によれば､発信端末は、位置情報と暗号化鍵を使って位置情報を暗号化する手段とを有し、定期的に（契約期限時には必ず）更新される暗号化鍵を使って位置情報を暗号化して着信端末に付属されたデコーダモジュールに送信する。デコーダモジュールは、発信端末の暗号化鍵更新時に自動更新される復号化鍵と、この復号化鍵を使って暗号化位置情報を復号化する手段とを有し、復号化された位置情報を着信端末に提供する。

【００１６】また、デコーダモジュールは、着信端末電話番号を保持する書き換え不可能な手段（ＲＯＭ）をもち、鍵更新時に着信端末電話番号を入れ込んだ鍵を生成しておくことで、発信端末で着信端末電話番号を入れ込んだ鍵を生成して位置情報を暗号化して送信したときに、デコーダモジュールで復号化して位置情報を得ることができる。

【００１７】図１は、本発明の第１の原理構成図であり、着信端末３は交換網７に直結され、着信端末３にはデコーダモジュール５が接続される。これに対し、図２に示された本発明の第２の原理構成図では、交換機７を介して発信端末１と着信端末３が接続され、デコーダモジュール５は、着信端末３と交換網７の間に接続される。

【００１８】請求項１に係る発明は、 交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおいて、上記発信端末１で、暗号化鍵及び上記着信端末３の識別情報を用いて上記位置情報を暗号化する段階と、上記発信端末１で、上記暗号化された位置情報を上記交換網７を介して上記着信端末３に送信する段階と、上記着信端末３に取り付けられ、上記暗号化鍵及び上記着信端末３の識別情報に対応した復号化鍵を保持するデコーダモジュール５で、上記着信端末３に受信された上記暗号化された位置情報を上記復号化鍵を用いて復号化する段階と、上記着信端末３で、上記復号化された位置情報を処理する段階とを有し、上記発信端末１の暗号化

鍵と上記デコーダモジュール５の上記復号化鍵が所定の時点で同期して更新され、上記デコーダモジュール５が取り付けられた着信端末において上記発信端末の位置情報を利用することができる位置情報利用方法である。

【００１９】請求項２に係る発明では、さらに、上記暗号化鍵を用いて位置情報を暗号化する段階は、上記暗号化鍵及び上記着信端末３の識別情報を用いてワーク鍵を作成する段階と、上記ワーク鍵を用いて上記位置情報を暗号化する段階とを有し、上記デコーダモジュール５に保持された上記復号化鍵は、上記更新された暗号化鍵及び上記デコーダモジュール５が取り付けられている上記着信端末３の識別情報を用いて更新される。

【００２０】請求項３に係る発明は、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムであって、上記発信端末１は、暗号化鍵及び上記着信端末の識別情報を用いて上記位置情報を暗号化する手段１２と、上記位置情報を記憶する手段１３と、上記暗号化鍵を所定の時点で更新する手段１４と、上記暗号化された位置情報を上記交換網を介して上記着信端末に送信する手段１１とを有し、上記着信端末３に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を保持する手段５３、上記着信端末３に受信された上記暗号化された位置情報を上記復号化鍵を用いて復号化する手段５１、及び、上記復号化鍵を上記暗号化鍵が更新される所定の時点で同期して更新する手段５２を備えたデコーダモジュール５が設けられ、上記着信端末３は上記復号化された位置情報を処理する手段３２を有し、上記デコーダモジュール５が取り付けられた上記着信端末３において上記発信端末の位置情報を利用することができる位置情報サービスシステムである。

【００２１】請求項４に係る発明は、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおける発信端末１の位置情報利用方法であって、暗号化鍵及び上記着信端末３の識別情報を用いて上記位置情報を暗号化する段階と、上記暗号化された位置情報を上記交換網７を介して上記着信端末３に送信する段階と、上記着信端末３に取り付けられ、上記暗号化鍵及び上記着信端末３の識別情報に対応した復号化鍵を保持し、上記暗号化された位置情報を上記復号化鍵を用いて復号化するデコーダモジュール５で、上記復号化鍵が更新される時点と同期して上記暗号化鍵を更新する段階とを有する、位置情報利用方法である。

【００２２】請求項５に係る発明によれば、上記暗号化鍵を用いて位置情報を暗号化する段階は、上記暗号化鍵及び上記着信端末３の識別情報を用いてワーク鍵を作成する段階と、上記ワーク鍵を用いて上記位置情報を暗号化する段階とを有し、上記デコーダモジュール５に保持された上記復号化鍵が上記更新された暗号化鍵及び上記デコーダモジュール５が取り付けられている上記着信端末３の識別情報を用いて更新される。

【００２３】請求項６に係る発明は、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおいて、暗号化鍵及び上記着信端末３の識別情報を用いて上記位置情報を暗号化する手段１２と、上記着信端末３に取り付けられ、上記暗号化鍵及び上記着信端末の識別情報に対応した復号化鍵を用いて、上記着信端末３に受信された上記暗号化された位置情報を復号化するデコーダモジュール５で上記復号化鍵が更新される所定の時点で同期して上記暗号化鍵を更新する手段１４と、上記暗号化された位置情報を上記交換網７を介して上記着信端末３に送信する手段１１とを有する発信端末である。

【００２４】請求項７に係る発明によれば、上記暗号化する手段１２は、上記暗号化鍵及び上記着信端末の識別情報を用いてワーク鍵を作成する手段と、上記ワーク鍵を用いて上記位置情報を暗号化する手段とを有する。

【００２５】請求項８に係る発明は、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおいて、上記発信端末１に搭載される位置情報利用プログラムを格納した記録媒体であって、暗号化鍵及び上記着信端末３の識別情報を用いて上記位置情報を暗号化させるプロセスと、上記着信端末３に取り付けられ、上記暗号化鍵及び上記着信端末３の識別情報に対応した復号化鍵を用いて、上記着信端末に受信された上記暗号化された位置情報を復号化するデコーダモジュール５で上記復号化鍵が更新される所定の時点で同期して上記暗号化鍵を更新させるプロセスとを有する位置情報利用プログラムを格納した記録媒体である。

【００２６】請求項９に係る発明によれば、上記暗号化させるプロセスは、上記暗号化鍵及び上記着信端末３の識別情報を用いてワーク鍵を作成させるプロセスと、上記ワーク鍵を用いて上記位置情報を暗号化させるプロセスとを有する。

【００２７】請求項１０に係る発明は、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおいて着信端末３に取り付けられたデコーダモジュール５の位置情報利用方法であって、上記発信端末１で暗号化鍵及び上記着信端末の識別情報を用いて暗号化され、上記交換網７を介して上記着信端末３に送信された暗号化位置情報を、上記暗号化鍵及び上記着信端末３の識別情報に対応した復号化鍵を用いて復号化する段階を有

し、上記発信端末１で上記暗号化鍵が更新される所定の時点で同期して、上記復号化鍵を更新する段階をさらに有する位置情報利用方法である。

【００２８】請求項１１に係る発明によれば、上記復号化鍵は、上記暗号化鍵及び上記着信端末３の識別情報を用いて作成されたワーク鍵を使って暗号化された上記暗号化鍵位置情報を復号化できるように、上記更新された暗号化鍵及び上記着信端末３の識別情報を用いて更新される。

【００２９】請求項１２に係る発明によれば、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおいて、着信端末３に取り付けられたデコーダモジュール５であって、上記発信端末１で暗号化鍵及び上記着信端末３の識別情報を用いて暗号化され、上記発信端末１に送信された暗号化位置情報を、上記暗号化鍵及び上記着信端末３の識別情報に対応した復号化鍵を用いて復号化する手段５１と、上記復号化鍵を保持する手段５２と、上記暗号化鍵が更新される所定の時点で同期して上記復号化鍵を更新する手段５３とを有するデコーダモジュールである。

【００３０】請求項１３に係る発明によれば、上記復号化鍵を更新する手段５３は、上記暗号化鍵及び上記着信端末３の識別情報を用いて作成されたワーク鍵を使って暗号化された上記暗号化鍵位置情報を復号化できるように、上記更新された暗号化鍵及び上記着信端末３の識別情報を用いて上記復号化鍵を更新する。

【００３１】請求項１４に係る発明は、交換網７と、上記交換網７を介して接続された発信端末１及び着信端末３とを有し、上記発信端末１の所在を表わす位置情報を上記着信端末３に提供する位置情報サービスシステムにおいて、着信端末３に取り付けられたデコーダモジュール５に搭載される位置情報利用プログラムを格納した記録媒体であって、上記発信端末１で暗号化鍵及び上記着信端末３の識別情報を用いて暗号化され、上記発信端末１に送信された暗号化位置情報を、上記暗号化鍵及び上記着信端末３の識別情報に対応した復号化鍵を用いて復号化させるプロセスと、上記暗号化鍵が更新される所定の時点で同期して上記復号化鍵を更新させるプロセスとを有する位置情報利用プログラムを格納した記録媒体である。

【００３２】請求項１５に係る発明によれば、上記復号化鍵を更新させるプロセスは、上記暗号化鍵及び上記着信端末３の識別情報を用いて作成されたワーク鍵を使って暗号化された上記暗号化鍵位置情報を復号化できるように、上記更新された暗号化鍵及び上記着信端末３の識別情報を用いて上記復号化鍵を更新させる。

【００３３】

【発明の実施の形態】図３は、本発明の第１の実施例の発信端末が鍵を更新し、位置情報を暗号化する処理を説明するための図である。

【００３４】発信端末は、最初に、所定の更新日時が到達したときに、記憶している現在（すなわち、更新前の）マスタ鍵と、この所定の日時を表す同期データとを用いて、マスタ鍵を更新し、更新後マスタ鍵を生成する。マスタ鍵の更新方法の一例として、現在マスタ鍵と現在時間を種として、乱数を発生し、発生された乱数を更新後マスタ鍵として使用する。乱数は、ＭＤ５、ＳＨ等の一方向性ハッシュ関数を乱数発生関数として用いることにより擬似的に生成することができる（“暗号理論入門”岡本栄治著、共立出版、Rivest, R.L. and Dusse, S. :The MD5 message-digest algorithm, Networking Group, INTERNET-draft, 1991）。鍵作成時にソースデータ（現在の鍵、時間など）を入力として、出力されたハッシュ値を更新されたマスタ鍵として使用することにより、マスタ鍵のランダム性が確保され、また、ソースデータの復元防止が実現されるので、マスタ鍵の偽造が阻止される。

【００３５】次に、マスタ鍵と、着信端末の識別情報、例えば、着信端末の電話番号を排他的論理和のような関数を用いて組み合わせて暗号化用ワーク鍵を生成する。したがって、発信端末では、着信端末毎に異なる暗号化用ワーク鍵を生成する。

【００３６】最後に、発信端末は、暗号化用ワーク鍵を用いて位置情報を暗号化し、暗号化位置情報を着信端末側のデコーダモジュールに供給する。図４は、本発明の第２の実施例のデコーダモジュールにおける鍵更新と、暗号化位置情報の復号化処理の説明図である。デコーダモジュールでは、発信端末と共通のマスタ鍵をデコーダモジュール内に保持し、発信端末とデコーダモジュールでそれぞれに保持しているマスタ鍵を同期的に更新させながら使用してもよいが、セキュリティ上、好ましくは、デコーダモジュールは、デコーダモジュールに固有のワーク鍵だけを記憶する。そこで、デコーダモジュールは、鍵更新処理の最初に、現在ワーク鍵から、現在（すなわち、更新前）マスタ鍵を再生する。マスタ鍵をワーク鍵から再生するためには、マスタ鍵からワーク鍵を作成する演算の逆演算を行う。そのため、デコーダモジュールが取り付けられている着信端末の電話番号と、現在ワーク鍵とを入力として、前述のワーク鍵生成の逆演算を実行する。

【００３７】次に、デコーダモジュールは、現在マスタ鍵と、発信端末側と同じ所定の更新日時を表す同期データとを用いて、前述の方法で更新後マスタ鍵を生成する。そして、更新後マスタ鍵と、着信電話番号とを用いて、復号化用ワーク鍵を生成する。この復号化用ワーク鍵は、次の更新処理の際に現在ワーク鍵として使用される。

【００３８】最後に、発信端末からの暗号化位置情報を

受けたデコーダモジュールは、復号化用ワーク鍵を用いて暗号化位置情報を復号化し、更なる処理に利用する。

【００３９】図５は、本発明の第３の実施例による鍵更新と位置情報送信の処理を全体的に示す図であり、図３及び４を参照して説明した発信端末側及びデコーダモジュール側の鍵更新方法及び暗号化方法が併せて示されている。

【００４０】着信端末に取り付けられるデコーダモジュールでは、着信電話番号をＲＯＭなどの記憶媒体に変更できないような形式で保持する。このため、デコーダモジュールは、定期締約などを締結している正規の着信端末以外の環境では正しく動作しない。

【００４１】以上の説明のように、本発明の実施例では、デコーダモジュールに着信電話番号を組み込み、埋め込まれた着信電話番号を使って生成されたワーク鍵が発信端末側で着信電話番号を使用して生成したワーク鍵と一致していなければ、デコーダモジュールで正しく復号化できない仕組みが提供される。そして、この仕組みと、マスタ鍵（すなわち、ワーク鍵）を定期的に更新する仕組みとを組み合わせることにより、契約した着信端末への着信に限定して復号化が可能であり、デコーダモジュールの転用が防止され、また、契約終了時にデコーダモジュールを回収することによって不正なサービス利用が阻止される。

【００４２】図６は、本発明の第４の実施例の位置情報サービスシステムのシステム構成図である。同図に示されたシステムは、交換網７００と、交換網７００に接続された複数ｎ台の発信端末１００$_1$、１００$_2$、．．．．、１００$_n$（以下の説明では、一般的に発信端末１００と表わす場合がある）と、着信端末３００と、着信端末３００に対応して取り付けられたデコーダモジュール５００とにより構成される。

【００４３】発信端末１００は、位置情報１３０と、暗号化のためのマスタ鍵１５０とを隠匿して保持し、発信時に位置情報１３０を暗号化する暗号化部１２０と、通常の電話機としての機能を実現し、暗号化された位置情報を送信する通信部１１０と、マスタ鍵１５０を定期的に更新する鍵更新部１４０とを有する。暗号化部１２０は、たとえば、図５に示されるように、マスタ鍵１５０と、着信端末の電話番号とを用いて、位置情報１３０を暗号化する。鍵更新部１４０は、たとえば、図５に示されるように、保存しているマスタ鍵１５０をデコーダモジュール５００と同期して定期的に更新する。また、発信端末１００は、時計１４１を有し、この時計１４１を用いてマスタ鍵の更新を行うためのタイミングを計る。この時計１４１は、後述のデコーダモジュール５００の時計と同期がとれているため、デコーダモジュールと同期して鍵の更新を行うことができる。電話交換網７００は、本例では、ユーザ間情報伝送を行う機能をもつネットワークである。着信端末３００は、通常の電話機能を実現すると共に、発信端末１００から送られてきた暗号化位置情報を、デコーダモジュール５００を使用して復号化し、得られた復号化された位置情報を表示する。着信端末３００の通信部３１０は、通常の電話機能を実行し、暗号化位置情報を受信したときには、暗号化位置情報をデコーダモジュールドライバ３３０に転送する。デコーダモジュールドライバ３３０は、通信部３１０から受け取った暗号化位置情報をデコーダモジュールに渡して、復号化を要求し、デコーダモジュール５００から復号化された位置情報を受信して、たとえば、表示ディスプレイに位置情報を表示させるため、復号化された位置情報を表示手段３２０に渡す。着信端末は、位置情報利用の一形態として、表示部３２０を有し、表示部３２０は、デコーダモジュール５００から受け取った位置情報を表示する。

【００４４】デコーダモジュール５００は、着信端末３００に接続されるハードウェアであり、着信端末３００から受け取った暗号化位置情報を復号化する復号化部５１０と、発信端末１００におけるマスタ鍵の更新と同期して、たとえば、図５に示されたようにワーク鍵５２０を定期的に更新する鍵更新部５３０とを有する。デコーダモジュール５００は、たとえば、RS-232C、USB、IEEE 1394等の任意の方式で着信端末３００と接続される。復号化部５１０は、図５に示されるように暗号化位置情報を受け取ると、ワーク鍵５２０を用いて位置情報を復号化し、着信端末３００に返す。鍵更新部５３０は、たとえば、図５に示された鍵更新方法に従って、発信端末１００と同期して一定期間毎に、更新前の現在のワーク鍵と、ユーザが書き換え不可能の形で保存されている着信端末電話番号とから、乱数発生関数などを使用して、ワーク鍵を更新する。また、時計５３１は、ワーク鍵の更新を行うためのタイミングを計り、発信端末１００の時計１４１と同期がとれている。

【００４５】典型的な例では、発信端末１００は公衆電話機のような電話機であり、着信端末３００はパーソナルコンピュータである。

【００４６】図７は、本発明の第４の実施例のシステムにおけるシーケンスチャートであり、以下、シーケンスチャートに沿って本システムの動作を説明する。

【００４７】まず、位置情報を知らせる発信者が発信端末で着信端末の電話番号をダイヤルする（ステップ１０１）と、発信端末の暗号化部は、マスタ鍵と着信端末の電話番号を使って位置情報を暗号化する（ステップ１０２）。発信端末は、着信端末に発呼して、暗号化された位置情報を送信する（ステップ１０３）。本実施例では、ISDN回線を利用し、Setup時にUUI［ユーザ・ユーザ・情報］で、この暗号化された位置情報を送信することができる。尚、ISDN回線以外であれば、モデム信号、DTMF信号、アウトチャンネル（音声帯域外）通信などで送信する。発信端末から送信された呼は、交換網を介して

着信端末に着信する（ステップ１０４）。

【００４８】着信端末は、暗号化位置情報を受けると、デコーダモジュールに転送する（ステップ１０５）。暗号化位置情報を受信したデコーダモジュールは暗号化位置情報を復号化し（ステップ１０６）、復号化された位置情報を着信端末に返送する（ステップ１０７）。着信端末は、復号化された位置情報を適当なフォーマットで表示する（ステップ１０８）。次に、着信端末で着信を受けて、着信者がオフフックし（ステップ１０９）、着信端末は交換網に応答信号を返信する（ステップ１１０）。応答信号を受けた交換網は、発信端末と着信端末の呼接続を行なう（ステップ１１１）。

【００４９】次に、本発明の第４の実施例のシステムの各装置における動作をプログラムとして構築した場合について、図８乃至１０のフローチャートを参照して説明する。

【００５０】図８は、本発明の第５の実施例の発信端末に搭載されるプログラムのフローチャートである。

【００５１】ステップ２０１）ユーザ（発信者）によりオフフックされた場合にはステップ２０２に移行し、そうでない場合にはステップ２０９）に移行する。

【００５２】ステップ２０２）ユーザが着信端末の電話番号を入力する。

【００５３】ステップ２０３）マスタ鍵と着信端末の電話番号を使い位置情報を前述の方法で暗号化し、暗号化位置情報を生成する。

【００５４】ステップ２０４）着信端末に発呼し、暗号化位置情報を送信する。このとき、ISDNであれば、セットアップ時にUUIで送信が可能であり、ISDN以外であれば、モデム信号、DTMF信号、アウトチャンネル通信などで送信するものとする。

【００５５】ステップ２０５）着信端末との接続に成功した場合には、ステップ２０６に移行し、そうではない場合にはステップ２１１に移行する。

【００５６】ステップ２０６）着信端末との通話を開始する。

【００５７】ステップ２０７）着信端末、又は、自端末からの切断要求が発行された場合、又は、オンフックされた場合にはステップ２０８に移行する。

【００５８】ステップ２０８）呼の切断処理を行なう。

【００５９】ステップ２０９）マスタ鍵更新のための所定の更新日時に達したかどうかを判定し、更新日時になった場合、ステップ２１０に移行し、そうでない場合にはステップ２０１に移行する。この所定の更新日時はデコーダモジュールに設定されている更新日時と一致している必要がある。

【００６０】ステップ２１０）前述の方法で発信端末が保持するマスタ鍵を更新する。

【００６１】ステップ２１１）着信端末との接続が失敗した場合にはエラー処理を行なう。

【００６２】図９は、本発明の第６の実施例の着信端末に搭載されるプログラムのフローチャートである。

【００６３】ステップ３０１）交換網を介して着信した場合にはステップ３０２に移行し、そうでない場合には待機する。

【００６４】ステップ３０２）位置情報を受信した場合にはステップ３０３に移行し、そうでない場合にはステップ３０６に移行する。

【００６５】ステップ３０３）暗号化位置情報を受信した場合には、暗号化位置情報を抽出、取得する。UUIで送信された場合には、Setupデータの中のUUIを解釈して、暗号化位置情報を取得する。

【００６６】ステップ３０４）暗号化位置情報をデコーダモジュールに転送し、デコーダモジュールで復号化された位置情報を獲得する。

【００６７】ステップ３０５）復号化された位置情報を着信端末のディスプレイに表示させる。

【００６８】ステップ３０６）着信があると着信音が鳴動する。

【００６９】ステップ３０７）発信端末との接続が成功したかどうかを判定し、成功した場合にはステップ３０８に移行し、そうでない場合にはステップ３１１に移行する。

【００７０】ステップ３０８）発信端末との通話を開始して、応答信号を発信端末に返却する。

【００７１】ステップ３０９）発信端末、若しくは、自端末からの切断要求、又は、オンフックが行なわれた場合に、ステップ３１０に移行し、そうでない場合、オンフックを待機する。

【００７２】ステップ３１０）呼の切断を行なう。

【００７３】ステップ３１１）発信端末との接続に失敗した場合には所定のエラー処理を行なう。

【００７４】図１０は、本発明の第７の実施例のデコーダモジュールに搭載されるプログラムのフローチャートである。

【００７５】ステップ４０１）着信端末から暗号化位置情報を受け取った場合にはステップ４０２に移行し、そうでない場合にはステップ４０４に移行する。

【００７６】ステップ４０２）ワーク鍵と着信端末電話番号とを用いて暗号化位置情報を復号化する。

【００７７】ステップ４０３）復号化された位置情報を着信端末に返信する。

【００７８】ステップ４０４）ワーク鍵を更新すべき鍵更新日時（例えば､毎月１日の午前０時）になった場合、ステップ４０５に移行し、そうでない場合にはステップ４０１に移行する。

【００７９】ステップ４０５）前述の方法でワーク鍵を更新する。

【００８０】ここまでの実施例では、デコーダモジュールは、発信端末から見た場合に、着信端末の下流側に接

続されている。例えば、デコーダモジュールがパソコンに実装されているような形態である。このようなデコーダモジュールの接続形態の場合、着信端末は、発信端末から送られてきた暗号化位置情報をデコーダモジュールに渡すと、復号化結果の位置情報がデコーダモジュールから返送される。これに対し、デコーダモジュールは、たとえば、ターミナルアダプタのように発信端末から見た場合に、着信端末の上流側に接続しても構わない。

【００８１】図１１は、本発明の第８の実施例のシステム構成図であり、デコーダモジュール５００は、ターミナルアダプタのような形で着信端末３００に接続されている。

【００８２】本実施例において、発信端末１００及び電話交換網７００は、図６に示された本発明の第４の実施例のシステムを構成する発信端末及び電話交換網と同じである。本発明の第８の実施例の場合、着信端末３００は、通信部３１０を備えた通常の電話機であり、選択的に、デコーダモジュールから通知された位置情報を利用するための位置情報処理部３２０を具備してもよい。

【００８３】デコーダモジュール５００は、上流側で電話回線に接続され、下流側で着信端末３００に接続される。デコーダモジュール５００と着信端末３００との間の接続は、たとえば、通常の電話機のインタフェースによって実現される。デコーダモジュール５００は、着信端末３００の発信時及び着信時に着信端末３００と電話交換網７００の間を取り次ぐ。さらに、デコーダモジュール５００は、通信部５４０で発信端末１００からの着信時に暗号化位置情報を受け取った場合には、復号化部５１０でワーク鍵５２０を用いて暗号化位置情報を復号化した後、位置情報利用部５５０で位置情報を表示する。また、デコーダモジュール５００は、鍵更新部５３０で、発信端末と同期して定期的にワーク鍵５２０を更新する。

【００８４】デコーダモジュール５００の通信部５４０は、上述のよ９うに、電話機のインタフェースを有し、着信端末３００の発着信時に着信端末３００と電話回線網７０とを中継し、発信端末１００からの着信時に暗号化位置情報を受け取った場合には、暗号化位置情報を復号化部５１０に渡す。位置情報利用部５５０は、復号化部５１０から受け取った位置情報を、ディスプレイに表示させたり、或いは、外部機器に送信する。復号化部５１０は、通信部５４０から暗号化位置情報を受け取ると、ワーク鍵を用いて位置情報を復号化し、復号化した位置情報を位置情報利用部５５０に渡す。鍵更新部５３０及び時計５３１については、図６を参照して説明した本発明の第４の実施例のシステムにおけるデコーダモジュールの鍵更新部及び時計と同じである。

【００８５】以上の説明では、発信端末の時計とデコーダモジュールの時計が一致している場合を考えている。しかし、何らかの原因で発信端末の時計とデコーダモジュールの時計に誤差が生じた場合、デコーダモジュールで復号化が不可能になることも考えられる。

【００８６】そこで、図１２に示された本発明の第９の実施例では、発信端末とデコーダモジュールの時計の誤差による問題（復号化不可能）を解決する復号化の正当性チェック機構について説明する。

【００８７】本実施例では、鍵更新が行われた後のある一定期間は、デコーダモジュール側で更新後の新ワーク鍵だけではなく、更新前の旧ワーク鍵を保持し使用できるようにする。この場合に、復号化時に新旧両方のワーク鍵を使用して復号化を行い（図１２の❶復号化及び❷復号化）、「復号化の正当性チェック手法」を用いて検証用データを使って復号結果を比較して（図１２の❹比較検証）、正しく復号化された方の位置情報を送信する（図１２の❺位置情報送信）。

【００８８】本実施例で適用される復号化の正当性チェック手法とは、デコーダモジュールで、記憶している着信電話番号を使用して生成したワーク鍵を用いて暗号化位置情報を復号化したとき、適切な位置情報フォーマットで復号化できたときに復号化が成功していることが検証される手法である。

【００８９】復号化が成功したこと、すなわち、適切な位置情報フォーマットで復号化できたかどうかは、デコーダモジュールで保存している検証用データと、デコーダモジュールで生成されたワーク鍵を用いた復号化によって取得された検証用データとを比較し、検証用データが一致したかどうかによって判定される。本発明の第８の実施例では、復号化の正当性チェックを、新ワーク鍵と旧ワーク鍵を用いた２通りの復号化によって取得された２通りの検証用データ（検証用データ１及び検証用データ２）について行い、正しい検証用データが得られた方の復号化によって得られた位置情報を選択し、着信端末に送信する。

【００９０】または、暗号化時に、位置情報データに対するチェックデジット等のチェックコードを位置情報データに付加し、復号化時に復号化された位置情報から算出したチェックコードと一致すれば復号化が成功したとみなす。

【００９１】図１３には、本発明の第９の実施例による復号化の正当性チェックのため暗号化位置情報に組み込まれた検証用データの例が示されている。同図の（Ａ）は位置情報フレームの形式を示し、（Ｂ）は種別番号の定義の例を示し、（Ｃ）は位置情報フレームの例を示す。「種別数」とは、フレーム中に含まれる位置情報種別の数を表す固定長データであり、「検証用データ」とは、復号化検証用のための固定データ又はチェックコードであり、「種別番号」とは、位置情報の種別を表す番号、すなわち、固定長データであり、「データ長」とは、データフィールドのオクテット数を表す固定長データであり、「データ」とは、種別毎の位置情報データで

あり可変長である。

【００９２】以上、本発明の代表的な実施例を説明したが、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【００９３】

【発明の効果】以上の説明の通り、本発明によれば、発信端末に位置情報を保持しているので、通信時に着信端末で位置情報を得ることができる。位置情報取得時に交換機網外で発信端末のＩＤ（電話番号）を使用しないので、発信端末のID（電話番号が）発信者・着信者の両方に秘匿される。また、復号化サービスを受ける着信者に確実に課金をすることができる。

【００９４】さらに、本発明によれば､着信端末として特番を使用しないので、着信端末が限定されない。位置情報は暗号化されているので、位置情報の改竄が防止できる｡その上、本発明によれば､発信端末は、位置情報と暗号化鍵を使って位置情報を暗号化する手段とを有し、定期的に（契約期限時には必ず）更新される暗号化鍵を使って位置情報を暗号化して着信端末に付属されたデコーダモジュールに送信する。デコーダモジュールは、発信端末の暗号化鍵更新時に自動更新される復号化鍵と、この復号化鍵を使って暗号化位置情報を復号化する手段とを有し、復号化された位置情報を着信端末に提供する。したがって、位置センタを利用しないので、復号化時の通信コストが低減され、かつ、鍵更新時にも通信コストが発生しないという利点が得られる。

【００９５】また、デコーダモジュールは、着信端末電話番号を保持する書き換え不可能な手段（ＲＯＭ）をもち、鍵更新時に着信端末電話番号を入れ込んだ鍵を生成しておくことで、発信端末で着信端末電話番号を入れ込んだ鍵を生成して位置情報を暗号化して送信したときに、デコーダモジュールで復号化して位置情報を得ることができる。これにより、契約した着信端末への着信に限定して復号化が可能であり、デコーダモジュールの転用が防止され、また、契約終了時にデコーダモジュールを回収することによって不正なサービス利用が阻止される。

【図面の簡単な説明】

【図１】本発明の第１の原理構成図である。

【図２】本発明の第２の原理構成図である。

【図３】本発明の第１の実施例の発信端末側暗号化処理の説明図である。

【図４】本発明の第２の実施例のデコーダモジュール側復号化処理の説明図である。

【図５】本発明の第３の実施例による鍵更新と位置情報送信の説明図である。

【図６】本発明の第４の実施例のシステム構成図である。

【図７】本発明の第４の実施例のシステムにおけるシーケンスチャートである。

【図８】本発明の第５の実施例の発信端末に搭載されるプログラムのフローチャートである。

【図９】本発明の第６の実施例の着信端末に搭載されるプログラムのフローチャートである。

【図１０】本発明の第７の実施例のデコーダモジュールに搭載されるプログラムのフローチャートである。

【図１１】本発明の第８の実施例のシステム構成図である。

【図１２】本発明の第９の実施例による復号化の正当性チェックの説明図である。

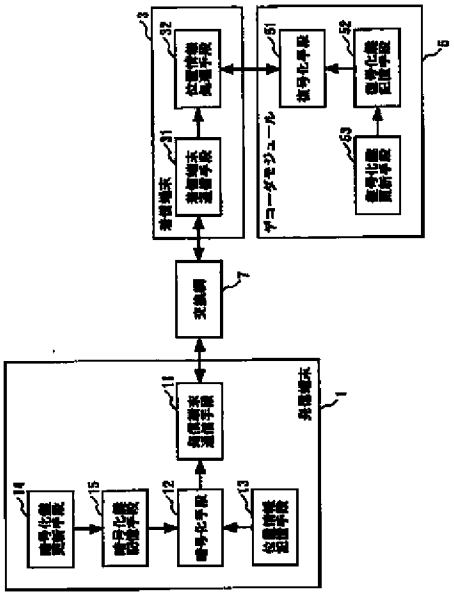
【図１３】本発明の第９の実施例の暗号化位置情報の例（検証用）

【符号の説明】

１　発信端末
３　着信端末
５　デコーダモジュール
７　交換網
１１　発信端末通信手段
１２　暗号化手段
１３　位置情報記憶手段
１４　暗号化鍵更新手段
１５　暗号化鍵記憶手段
３１　着信端末通信手段
３２　位置情報処理手段
５１　復号化手段
５２　復号化鍵記憶手段
５３　復号化鍵更新手段

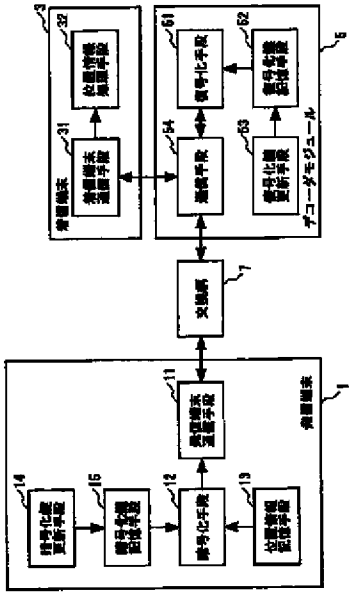
【図１】

本発明の第１の原理構成図



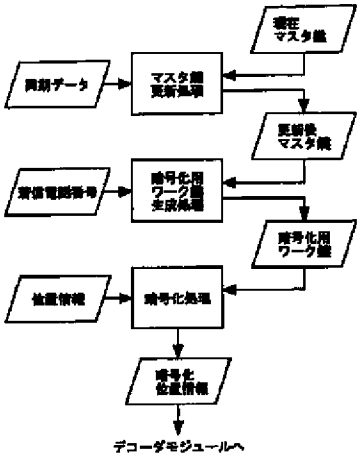
【図２】

本発明の第２の原理構成図



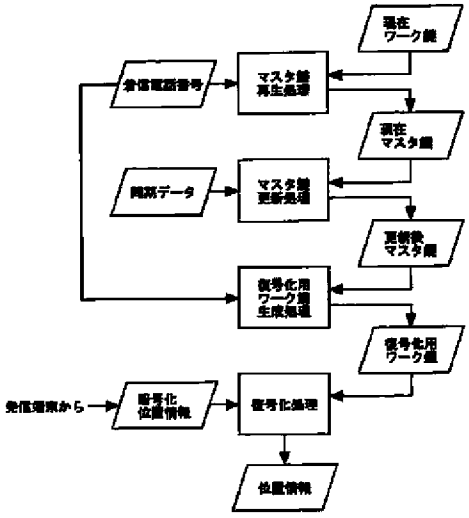
【図３】

本発明の第１の実施例の発信端末側暗号化処理の説明図



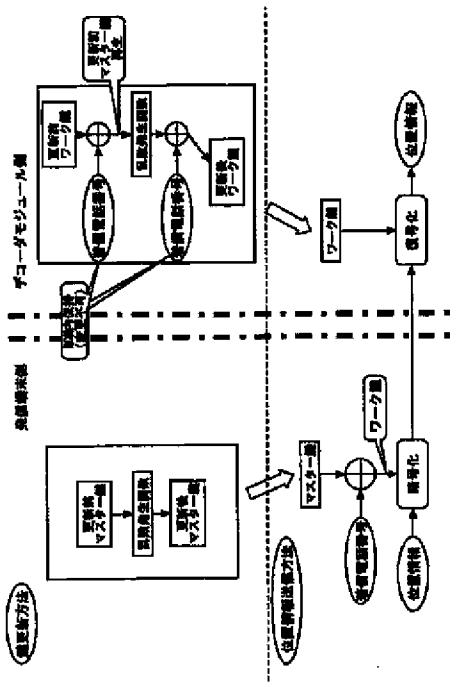
【図４】

本発明の第２の実施例のデコーダモジュール側復号化処理の説明図



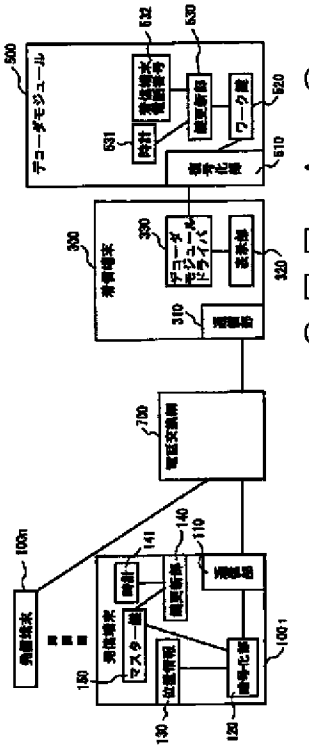
【図５】

本発明の第３の実施例による鍵更新と位置情報送信の説明図



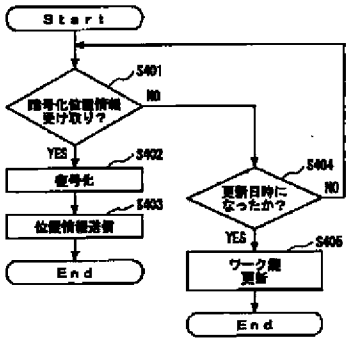
【図６】

本発明の第４の実施例のシステム構成図



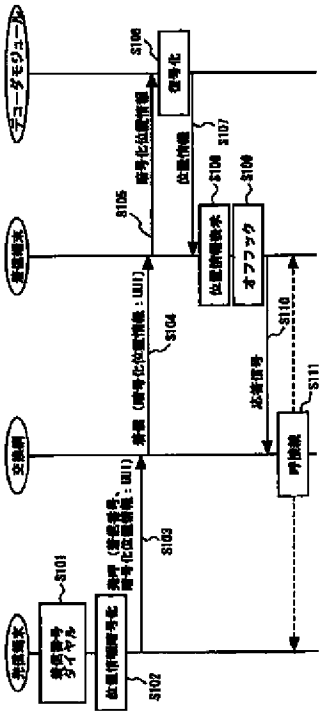
【図１０】

本発明の第７の実施例のデコーダモジュールに搭載されるプログラムのフローチャート



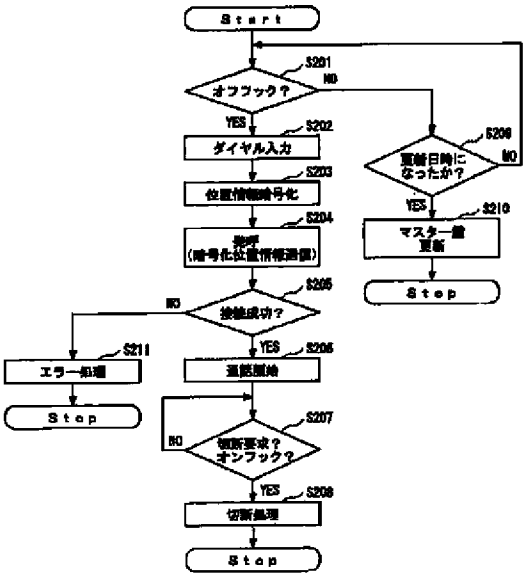
【図７】

本発明の第４の実施例のシステムにおけるシーケンスチャート



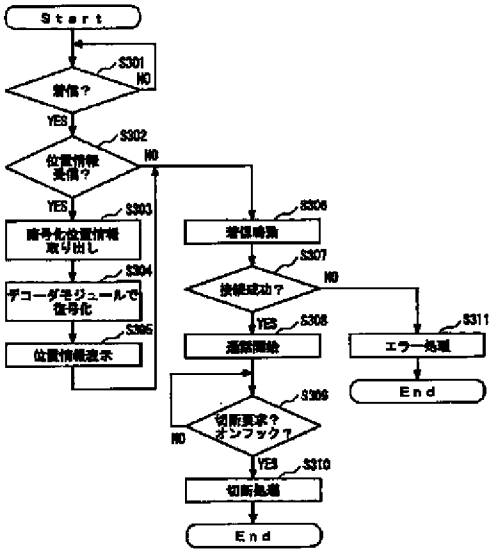
【図８】

本発明の第５の実施例の発信端末に搭載されるプログラムのフローチャート



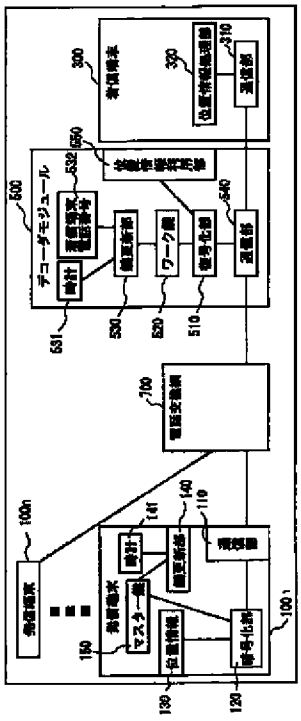
【図９】

本発明の第６の実施例の着信端末に搭載されるプログラムのフローチャート



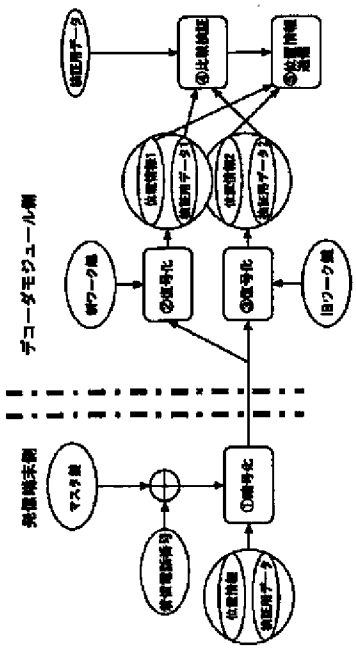
【図１１】

本発明の第８の実施例のシステム構成図



【図１２】

本発明の第９の実施例による復号化の正当性チェックの説明図



【図１３】

本発明の第９の実施例の暗号化位置情報の例（検証用）

（Ａ）暗号化位置情報フレーム

種別数(n)	検証用データ	
種別番号１	データ長１	データ１
⋮	⋮	⋮
種別番号ｎ	データ長ｎ	データｎ

（Ｂ）種別番号定義の例

種別	種別番号
緯度・経度	1
住所	2
郵便番号	3
マップコード	4
カスタマイズ情報 (ビル名・階数・電話番号等)	5

（Ｃ）暗号化位置情報フレームの例

検証用データ例

3	11010011101100010111010100	
1	26	E.139.40.00.0,N,35.13.15.2
2	28	神奈川県横須賀市光の丘１－１
5	32	ＮＴＴ横須賀研究開発センタ 320C

フロントページの続き

(72)発明者　安永　健治
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　嶺　真一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA01 AA16 BA01 EA02 EA06 EA26 NA03 NA05 NA27 PA07
5K015 AE05 AF06
5K024 AA71 DD01 DD06 GG01 GG10
5K101 KK16 LL01 NN21 PP03